SMP Gateway Malware Protection

NERC CIP-007 R4 requires the use of anti-virus software and other malicious software ("malware") prevention tools to detect, prevent, detect, and mitigate the introduction, exposure, and propagation of malware on all Cyber Assets within the Electronic Security Perimeter.

This document describes how the **Cooper Power Systems' Cybectec SMP Gateway** implements malware protection.

In this document

Quebec City
730 Commerciale Street
Suite 200
Saint-Jean-Chrysostome, Quebec
Canada G6Z 2C5
Phone: +1.418.834.0009
Fax: +1.514.227.5256

Montreal
1290 St. Denis Street
Suite 300
Montreal, Quebec
Canada H2X 3J7
Phone: +1.514.845.6195
Fax: +1.514.227.5256

www.coopoerpowereas.com

2009/10/15

Introduction

Malware is the generic term used to describe the various forms of malicious software programs such as viruses and worms that are inserted into a system, usually without the knowledge of the user, with the intent of compromising the confidentiality, integrity, or availability of the victim's data, applications, or operating system.

Protecting a system against malware requires a defense-in-depth strategy where the last level of protection is typically provided by an antivirus application. The anti-virus application scans all files on a system in the search of known malicious patterns in executable code, isolates these files, and prevents their execution.

To be effective, an antivirus requires an up-to-date database of malicious patterns, known as virus signatures. Maintaining such a database is rapidly becoming a challenge because of the growing number of new attacks. Symantec detected 1,656,227 malicious code threats in 2008, representing over 60 percent of the approximately 2.6 million it has detected in total over time[1]. Even with up-to-date information, an antivirus offers no protection against new threats, also called "zero-day exploits", until the virus is identified and a signature becomes available.

Protecting embedded control systems introduces additional challenges. Performance is critical, disk and memory capacity is limited. Furthermore, for security reasons these systems need to be isolated from the Internet or the enterprise network, making the retrieval of updated virus signatures quite difficult.

Using Application Whitelisting to Protect Against Malware

An antivirus scans executable files and prevents known malware from executing. This strategy ensures good malware protection for "open" systems used in an enterprise setting where users download files from the Internet and receive email attachments.

The situation is quite different with embedded and process control systems where the software configuration is generally "locked down". Software is installed and configured during system commissioning and generally remains the same until there are scheduled maintenance and updates.

This difference in the system lifecycle justifies a different malware prevention strategy. Instead of blocking the execution of software that appears in a list of "blacklisted" applications, it is much more effective to maintain a list of applications that are allowed to run on the system and prevent everything else. This technique, called "whitelisting", provides the best protection for embedded systems where the software configuration is known in advance and rarely changes.

Valid executable files can be identified in different ways. The operating system can keep a list of files that are safe to execute. However, this approach is vulnerable if the file list is compromised. Furthermore, an attacker could replace a valid file by another file with the same name.

Cooper has chosen to mark each executable file in the SMP Gateway with a digital signature, or fingerprint, which ensures its authenticity and guarantees its integrity.

---

[1] *Symantec Global Internet Security Threat Report Trends for 2008*, Volume XIV, Published April 2009

SMP Gateway Software Validation Process

SMP Gateway Software Components

The SMP Gateway software is composed of the following major executable modules:

- The bootstrap loader
- The Windows CE operating system
- The gateway application

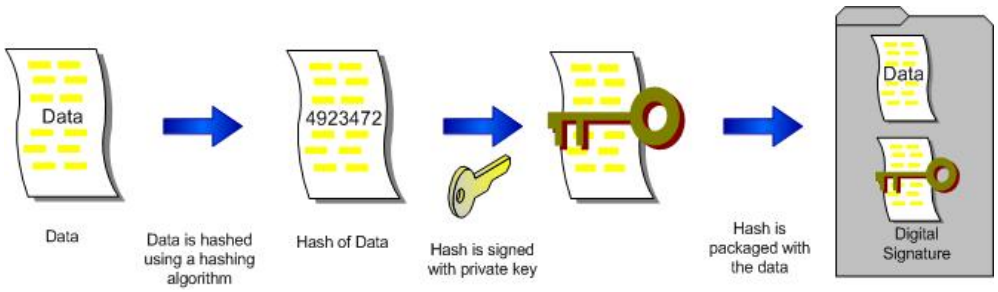
Each of these modules may itself be composed of a number of components in the form of EXE or DLL executable files. The Cooper software validation ensures the authenticity and integrity of all these files.

File Signing

Each SMP Gateway EXE or DLL executable file is signed using a digital signature that guarantees the identity of the issuer and ensures that the file was not modified. The digital signature algorithm uses a cryptographic hash function and a private/public key pair, also known as asymmetric encryption.

To sign a file, the issuer calculates a unique value, similar to a checksum, based on the file contents. The hashing algorithm is selected so that any change in the file contents will result in a different hash value. Cooper uses the SHA-1 hashing algorithm.

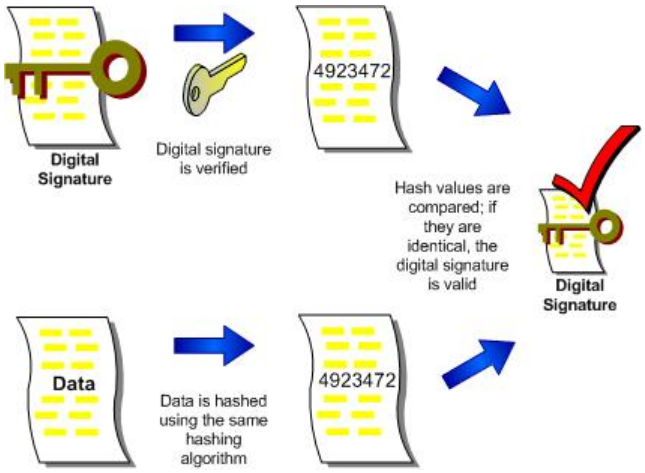
The hashed value is then encrypted using the RSA algorithm and a private encryption key unique to Cooper. The encrypted file hash value constitutes the file signature.



Creating a Digitally Signed File[2]

To validate a file, the SMP Gateway uses the Cooper public key to decrypt the file signature. It then calculates the file hash using the same hashing function as the issuer. If the file contents are authentic and have not changed, this value will be the same as the decrypted hash accompanying the file.

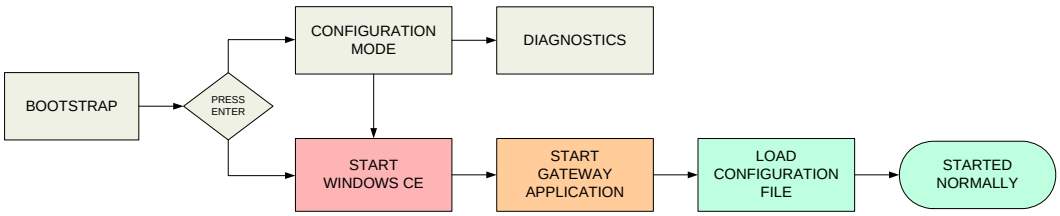
[2] *Code Signing Best Practices*, Microsoft, July 25, 2007.



Verifying a Digital Signature[3]

The SMP Gateway Startup Cycle

At system startup, the SMP Gateway goes through the steps illustrated below.



SMP Gateway Startup Cycle

When it starts, or after a reset, the SMP Gateway launches the **bootstrap loader**.

The bootstrap loader prompts the user to enter Configuration Mode. If the user does not press ENTER within 15 seconds, the bootstrap loads the **Windows CE Operating System**. The operating system is stored as a single archive file in the SMP Gateway FLASH memory. The bootstrap extracts each EXE and DLL component from the archive and copies it to the system RAM memory. Once the components of Windows CE are loaded in RAM, the bootstrap starts the operating system. The Windows operating system protects its components and prevents a component already loaded in memory from being replaced until the system is restarted.

Windows CE first launches the **Integrity Scan** process, which is described later in this note, to ensure that all files on the SMP Gateway are valid.

---

[3] *Code Signing Best Practices*, Microsoft, July 25, 2007.

Windows CE then launches the **Gateway Application**. This application provides all the functionality of the gateway: communications, protocol handling, automation functions, passthrough, etc.

Finally, the Gateway Application loads the **Configuration File** and starts processing data.

Protecting Software Components

In order to ensure the integrity of SMP Gateway software components, Cooper uses authentication, encryption and code signing.

The SMP Manager application uses Transport Layer Security (TLS, previously known as SSL) to communicate with the gateway. The TLS protocol uses the SMP Gateway built-in certificate to ensure that both the SMP Gateway and SMP Manager are legitimate. TLS then sets up an encrypted communication channel with the gateway.

When SMP Gateway authentication is activated, only authorized users can connect to the gateway. SMP Manager forwards the user credentials to the gateway before all operations. The SMP Gateway validates the user credentials, assigns permissions and allows or prohibits the requested operation.

Authorized users can then use the following commands from the SMP Manager **Update** menu to securely manage files on the SMP Gateway.

- **Update SMP Gateway Firmware** – this command is used to update the bootstrap loader and the Windows CE operating system. Its use is limited to users with the **System Management** access permission. The command validates the file signature and can only be used to send a file issued by Cooper to the SMP Gateway. Any other file will be rejected.
- **Update SMP Gateway Application** – this command is used to update the gateway application. This component contains all the SMP Gateway application modules including protocols and licensed options. Its use is limited to users with the **System Management** access permission. The command validates the file signature of each module and can only be used to send modules issued by Cooper to the SMP Gateway. Any unsigned module will be rejected.
- **Send File** – this command is used to send special data files to the SMP Gateway, such as an appropriate use banner, event file processing templates and CoDeSys scripts. Use of the command is limited to users with the **System Management** access permission. The command validates the signature of Windows executable EXE or DLL files and can only be used to send modules issued by Cooper to the SMP Gateway. Any unsigned module will be rejected.
- **Send Configuration File** – this command is used to send system configuration files to the SMP Gateway. Use of the command is limited to users with the **Configuration** access permission.

Notes:

Besides the commands described above, there are only two other ways to load or modify a file on the SMP Gateway:

- Users with the **System Management** access permission can use the **SMP Console** application to copy, delete and rename files on the SMP Gateway. This tool must be used with care as it can render the gateway unusable. Any

executable file modified through this tool would be identified by the **Integrity Scan** function described in the next section.

- Some protocols provide file transfer capabilities. These files are generally copied to specific data areas. In the event that a malicious party discovered a means to load an executable file loaded through this capability, it would be identified by the **Integrity Scan** function described in the next section.

Integrity Scan

As described in the previous section, the SMP Manager prevents users from loading invalid executable files on the SMP Gateway. However, no system can claim to be totally secure. A malevolent party could discover a vulnerability and exploit it to load or modify a file on the SMP Gateway.

To protect against this occurrence, the SMP Gateway continuously runs an **Integrity Scan** as a background process that checks the signature of each executable file in the system to protect against any type of data corruption resulting from hardware or software failure, or tampering.

If an invalid executable file is detected, the SMP Gateway records the name of the file in the security log, and puts itself into a safe mode in which it interrupts all communication with devices and control centers.

SMP Tools can be used to manage an SMP Gateway in safe mode, to access the logs, view and retrieve files, and ultimately restore the system components.

Conclusion

Signature-based antivirus solutions are designed to identify known malware and stopping it before it executes. Unless the antivirus solution implements very sophisticated platform-specific algorithms, it cannot protect a system from a zero-day exploit.

Cooper has thus chosen a different strategy to protect the SMP Gateway from malware. The only way an authorized user can load files on the gateway is through the use of the SMP Tools applications provided with the gateway. These tools prevent users from loading anything but original executable files signed by Cooper.

If a malicious party did find a way to load a foreign executable file by exploiting a vulnerability, an Integrity Scan process will detect it and stop the compromised gateway.

Combined, these functions effectively protect the SMP Gateway against malware in an operational environment where signature-based antivirus solutions are not available, or are not appropriate because they cannot be effectively maintained. The solution provides the additional benefit of detecting data corruption resulting from hardware or software failure.